VX-AP450N 802.11n Wireless High Power Ceiling Access Point

Revision 1.0

User Manual

2010-11-24

Contents

Chapter 1 Product Overview……..……..……..3
1.1 Product Features……..……3
1.2 Package Contents……..……3
Chapter 2 Product Installation……..……..……4
Chapter 3 Configuration Guide……..……..…..5
3.1 WebLogin……..……5
3.2 Setup Wizard……..……..6
3.3 Wireless AP (AP) Mode……..……...6
3.4 Bridge (WDS) Mode ……..……7
3.5 System Status ……..……10
3.6 LAN Settings ……11
Chapter 4 Wireless Settings……..……...12
4.1 Basic Settings……..……12
4.1.1 Access Point (AP) Mode……..12
4.1.2 Bridge (WDS) Mode…..……14
4.2 Security Settings ……..……18
4.2.1 AP Security Setting ……18
4.2.2 WDS Security Setting……..……...25
4.3 Advanced Settings……...25
4.4 Access Control…..……26
4.5 Connection Status……..……...27
Chapter 5 SNMP Configuration……..……..28
5.1 SNMP Introduction……...28
5.2 SNMP Setting……28
Chapter 6 SystemTools……..……..……30
6.1 Change Password……30
6.2 Restore to Factory……..30
6.3 Backup/Restore……..……31
6.4 Time Settings……..……..…32
6.5 Reboot…..……..……32
6.6 Firmware Upgrade……..……33
6.7 System log……33
Appendix I: Glossary……..……35
Appendix II: TCP/IP Address Setting (Take Windows XP for example)……..36
Appendix III: WDS Application Instances……..……39

Chapter 1 Product Overview

This wireless indoor
AP is an advanced ceiling AP based on 802.11n standard with 300Mbps data rate using MI MO (Multiple In & Multiple Out) technology to increase coverage. There are 4 operation mo des and strong security mechanism for various application demands.

1.1 Product Features

- Wireless LAN 802.11n & 802.11b/g compliant
- Multi-function: AP, Repeater & WDS
- 300Mbps (2T2R)
- Advanced MIMO technology
- Gigabit Auto-negotiation LAN port supported for LAN connection
- Support power adapter & POE
- WebUI management interface
- Powerful network security: 64/128-bit WEP encryption, WPA and WPA2
- Auto MDI/ MDIX
- Support SNMP & VLAN pass through
- Watchdog function

1.2 Package Contents

The following items are included in the package:

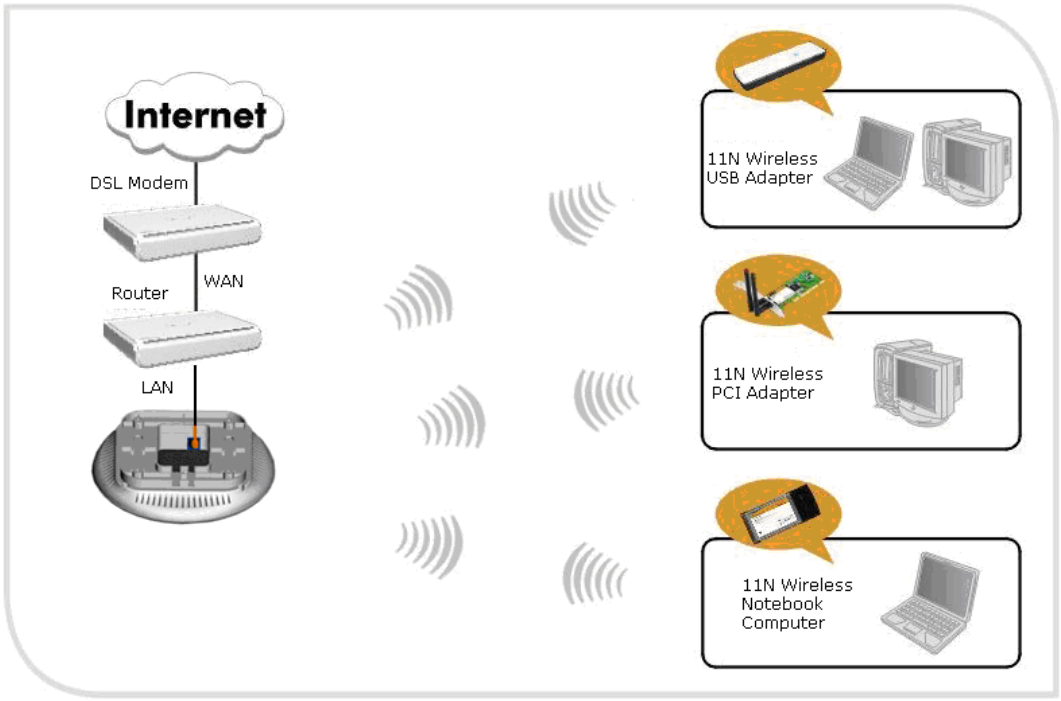
- Wireless Ceiling AP *1
- Power Adapter or PoE & Power Cord *1
- Screws *4
- Network Cable *1
- Plastic wall-plugs *4

Note: If any of listed items are missing or damaged, please contact the reseller from whom you purchased for replacement immediately.

Chapter 2 Product Installation

It is highly recommended to install this ceiling AP after configuration based on the instructions in chapter 3.

The basic topology is as below:



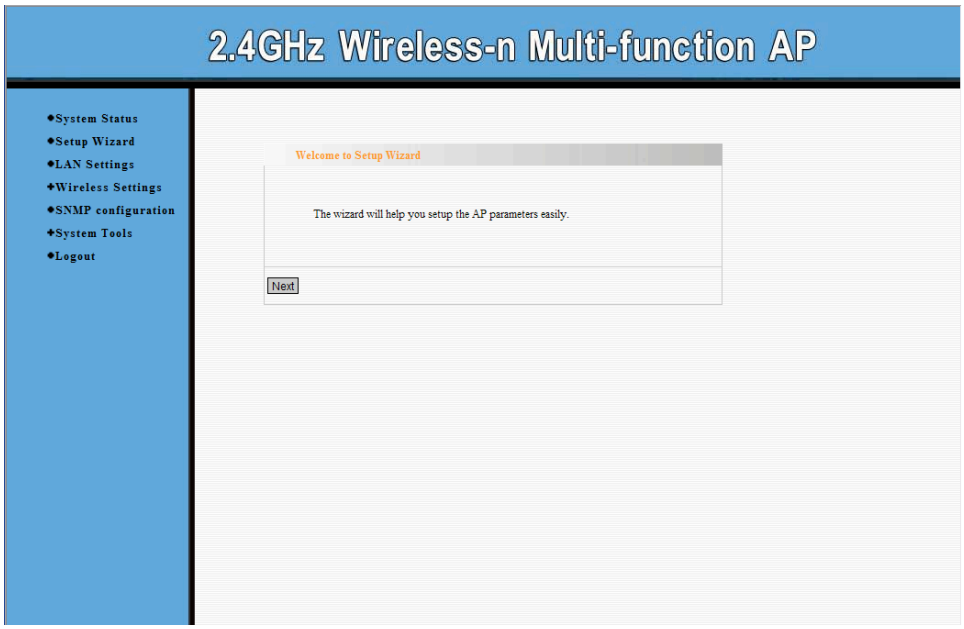
Chapter 3 Configuration Guide

3.1 Web Login

Connect to ceiling AP via wired cable and configure 192.168.0.x (x ranges 2-254) as the IP address on your PC, and 255.255.255.0 as subnet mask (Please refer to the Appendix II for details on TCP/IP setting).

Launch Internet Explorer; enter the default IP address as 192.168.0.254. Press enter and the login screen will appear. Enter admin for both **User name** and **Password**.

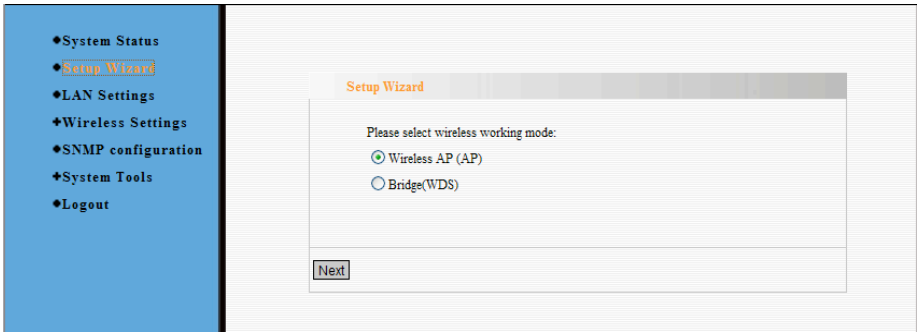
Click **OK** to enter the main page.



You can select **System Status**, **LAN Settings**, **Wireless Settings**, **SNMP configuration** and **System Tools** on the left menu for details. Click **Next** to enter the wireless operation mode setup page. Ceiling AP supports two working modes: **Wireless AP (AP)** and **Bridge (WDS)**. Select a working mode to configure the settings. For more details, please refer to the following chapters.

3.2 Setup Wizard

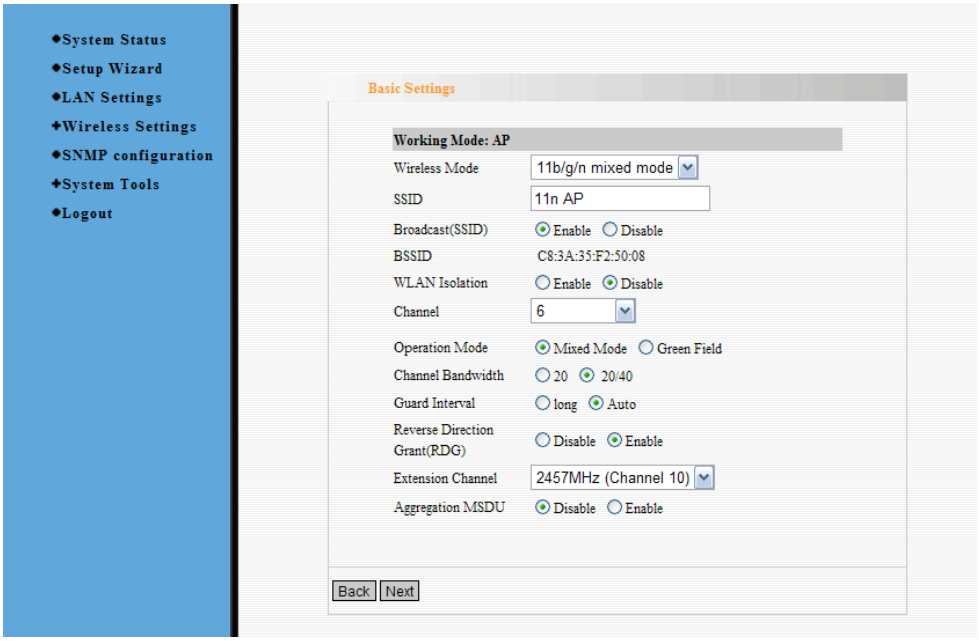
This is a convenient tool that you can easily complete basic settings of ceiling AP. Click **Next** in the first page and it will guide you through the settings.



On this page, you can select **Wireless AP (AP)** or **Bridge (WDS)** to adapt different wireless access environment.

3.3 Wireless AP (AP) Mode

Select **Wireless AP (AP)** and click **Next** to enter the basic settings.



Enter proper information in this page

1. **SSID:** Set the SSID of the device.
2. **Channel:** Select the wireless communication channel. The default is channel 6.

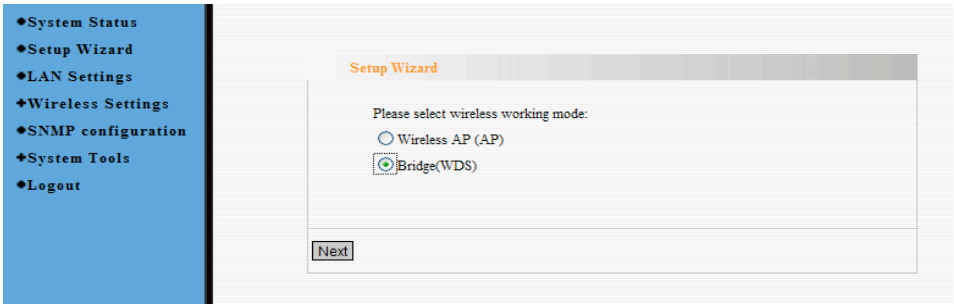
After you finish the settings, click **Next** to enter the **AP Security Settings** page as the picture below:

AP Security Settings is used to encrypt the settings for ceiling AP and authorize the wireless client to access the AP for security in wireless network. Please refer to **Chapter 4.1.1.2** for detailed security setting specifications.

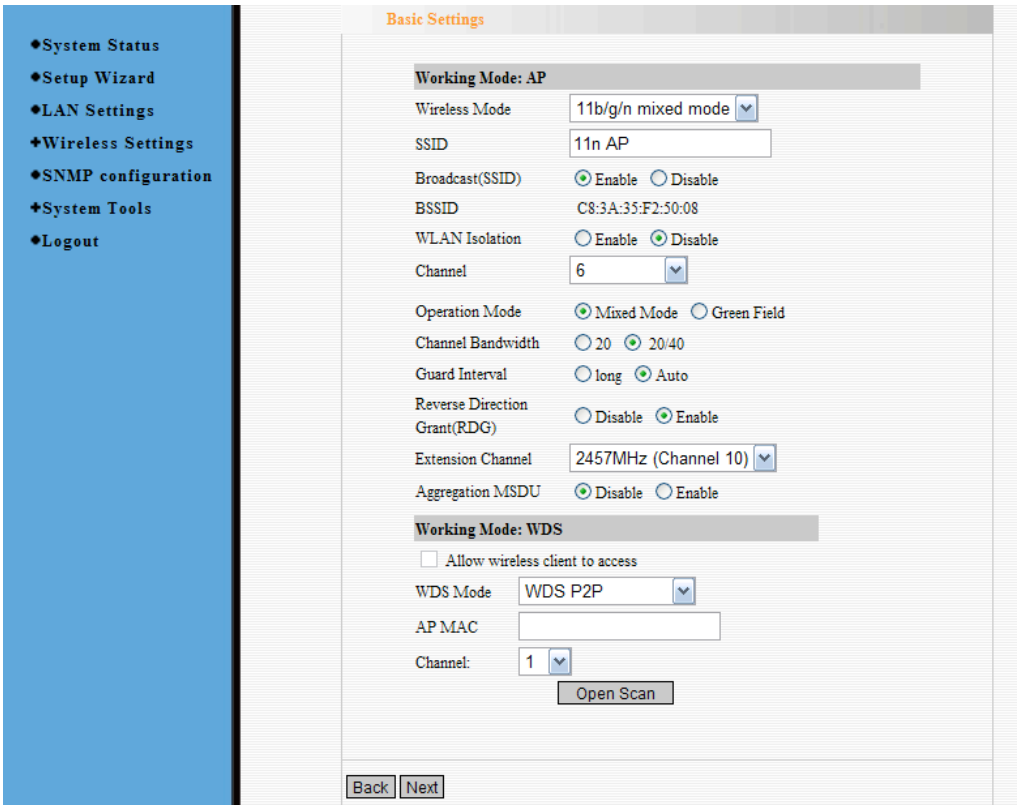
After finishing the settings, click **Next** to finish settings as the picture below.

3.4 Bridge (WDS) Mode

Select **Setup Wizard** on the left menu and the working mode selection will appear as the picture below.

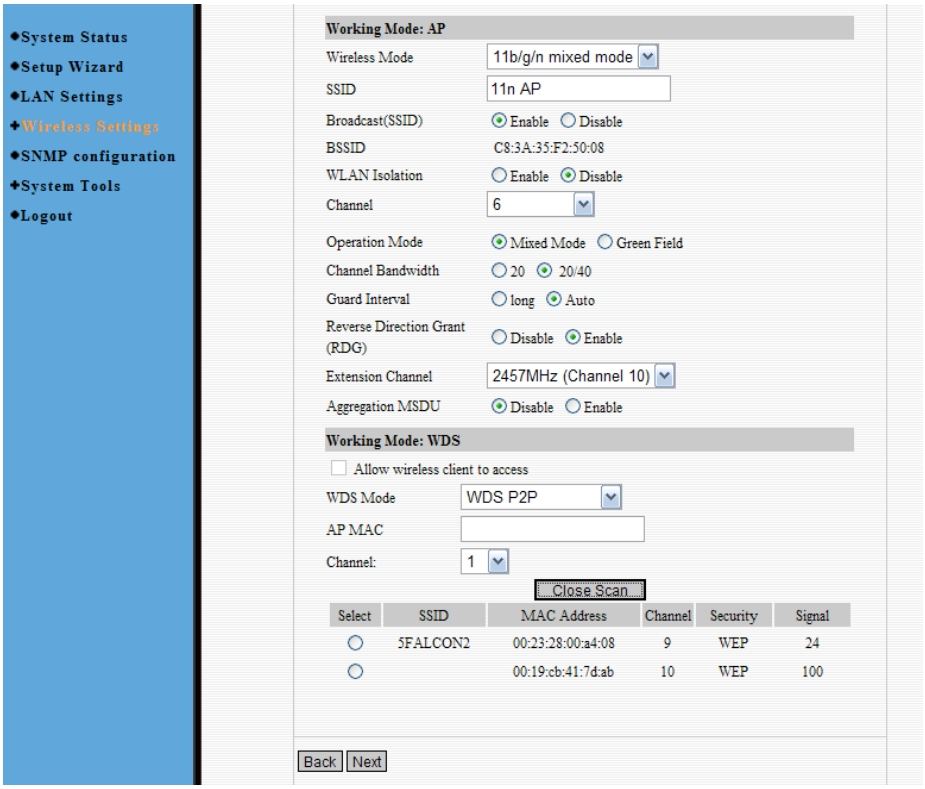


Select **Bridge (WDS)** and click **Next**. You will enter the **WDS** setup page as the picture below.

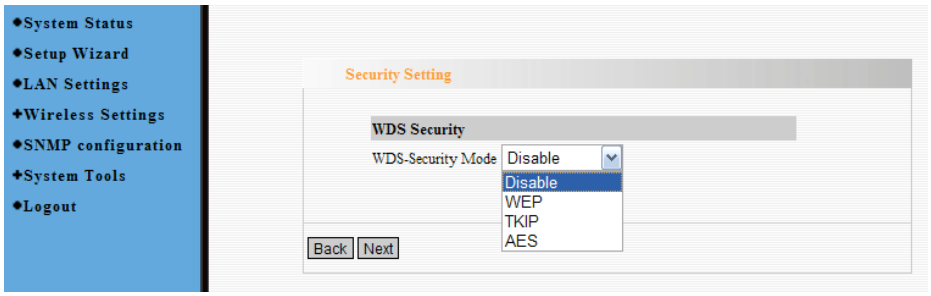


Bridge (WDS) working mode includes: Point-to-Point Bridge (**WDS P2P**), Point-to-Multipoint Bridge (**WDS P2MP**), Wireless Repeater (Repeater).Users can select the mode according to need. Please refer to **Chapter 4.1.2** for detailed introduction.

Then click **Open Scan**, ceiling AP will scan and list all the available wireless device nearby automatically (see the picture below). Select the ceiling AP which you need to bridge and click **Next** to enter the **WDS Security** setup interface. On the other hand, you can enter the MAC address of wireless device which you want to bridge manually and select the corresponding channel.

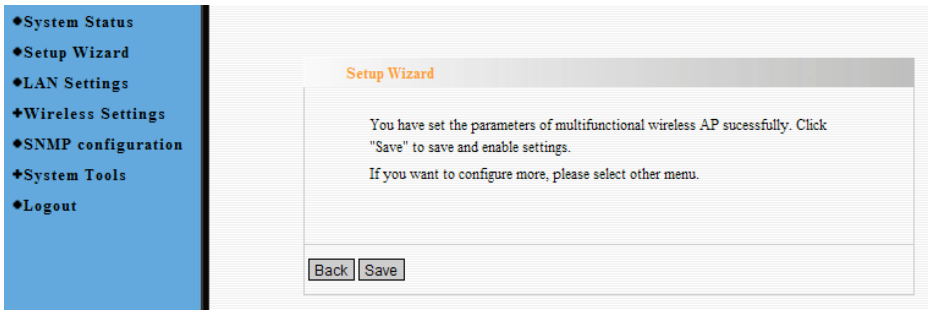


After finish the settings, click **Next** to enter the **WDS Security** setting option as the picture below.



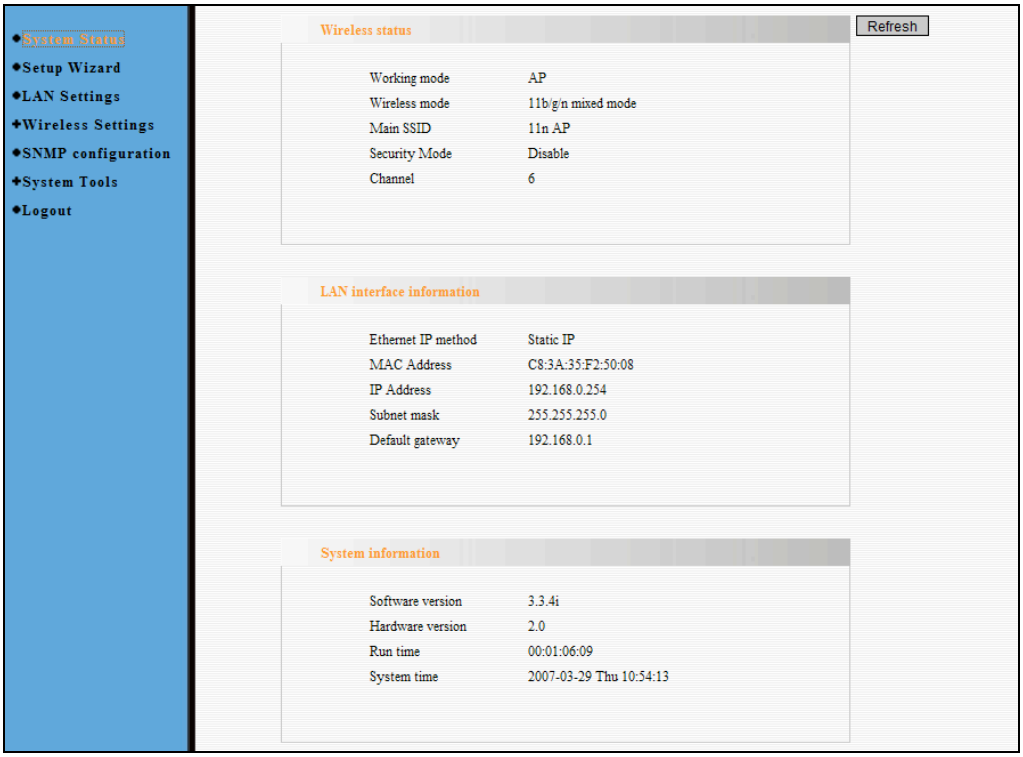
WDS Security setting is used to encrypt the ceiling AP and authorize the device to establish bridge connection. Only when the passwords of the devices in bridge are consistent, the communication can get through normally.

After finishing all the settings, click **Next** and **Save**.



3.5 System Status

This page shows the current status of ceiling AP, including **Wireless status**, **LAN interface information** and **System information**.



- ***Wireless status***

  It shows the current working status, including working mode, wireless mode, main SSID, security mode and channel.

- ***LAN interface information***

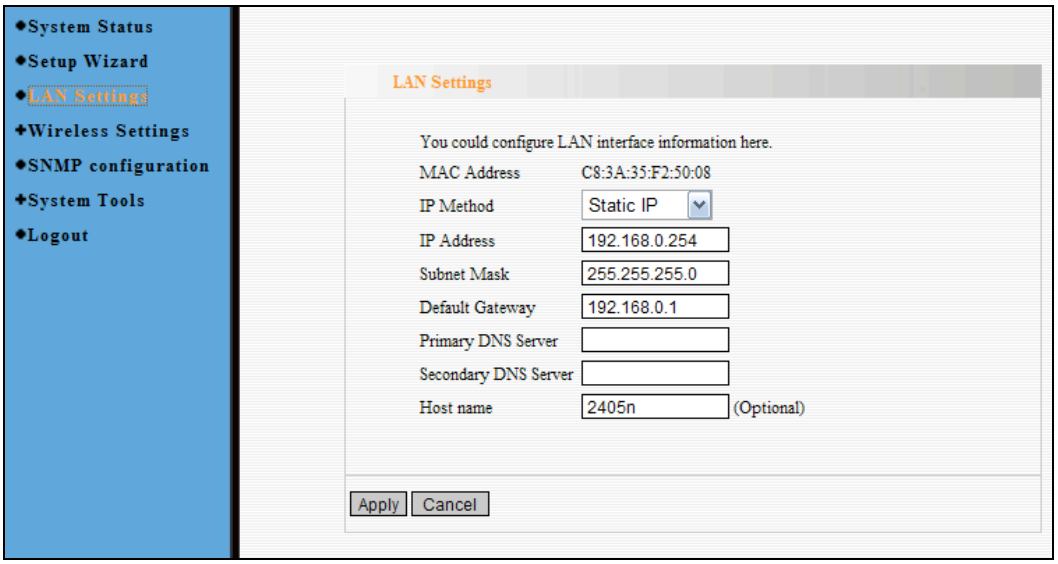
  It shows how LAN IP is obtained, MAC address, IP address, subnet mask etc.

- ***System information***

  It shows the current software version, hardware version etc.

3.6 LAN Settings

This section mainly deals with LAN's basic settings.



- ***Static IP:*** The default IP address is 192.168.0.254. You can configure a new IP address, subnet mask and gateway manually for the device, if necessary
- ***Dynamic IP:*** Automatically obtain IP address, subnet mask and gateway from DHCP server (unless you have permission to obtain this information from the uplink connected device, otherwise, it is not recommended to select this way).

Note: If the LAN IP address is changed, you need to use the new IP address to login ceiling AP Web interface next time.

Chapter 4 Wireless Settings

This chapter introduces you wireless settings in two working modes: Access Point (AP) and Bridge (WDS), including basic settings, security settings, advanced settings, access control, and connection status.

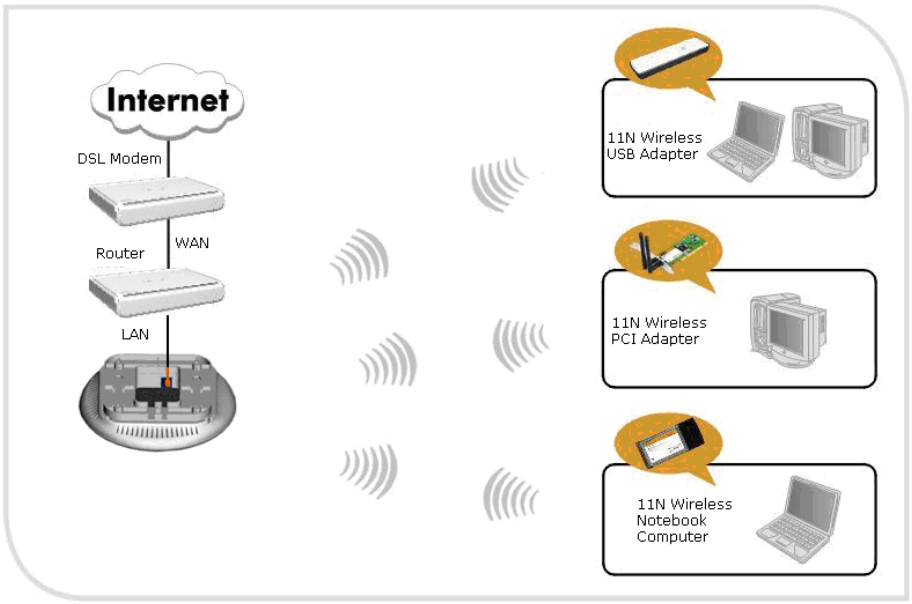
4.1 Basic Settings

Access Point (AP) Mode:

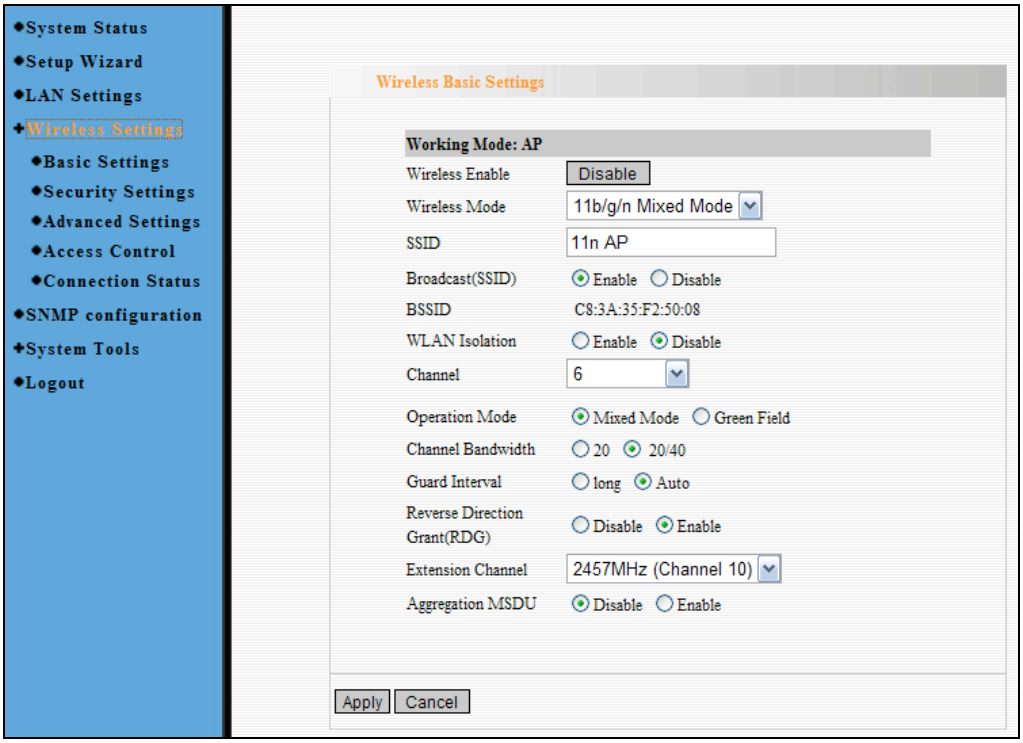
In this mode, ceiling AP will act as a central hub for accesses from wireless to wireless, wireless to wired, and wireless to WAN. The most important is to provide a wireless client access such as wireless network adapter access.

4.1.1.1 Application and Topology Plan

The AP mode can convert the wired transmission into wireless signals. If you have one wired cable connecting to Internet, and want to access the Internet via wireless signals connecting to your notebook computer, this mode fits perfectly.



4.1.1.2 Function Explanation



- ***Wireless Enable:*** Click **Disable** to turn off all the wireless feature of this ceiling AP; click **Enable** to open the wireless feature.
- ***Wireless Mode:*** Select one of the following modes. The default is **11b/g/n Mixed Mode**.
- ***11b Mode:*** Allow the wireless client to connect the ceiling AP in 11b mode at the maximum speed of 11Mbps.
- ***11g Mode:*** Allow the 11g/11n-compliant client device to connect the ceiling AP at the maximum speed of 54Mbps.
- ***11b/g Mixed Mode:*** Allow the 11b/g-compliant client device to connect the ceiling AP with auto-negotiation speed, and 11n wireless client to connect the ceiling AP with 11g speed.
- ***11b/g/n Mixed Mode:*** Allow 11b/g/n-compliant client device to connect the ceiling AP with auto- negotiation speed. The maximum speed is 300Mbps.
- ***SSID:*** SSID (Service Set Identifier) is the unique name of the wireless network. It is recommended to modify this name for wireless client to recognize wireless signals.
- ***Broadcast (SSID):*** When you select **Disable**, ceiling AP will not broadcast its own SSID number. If there is a wireless connection request, you need to input SSID number manually.

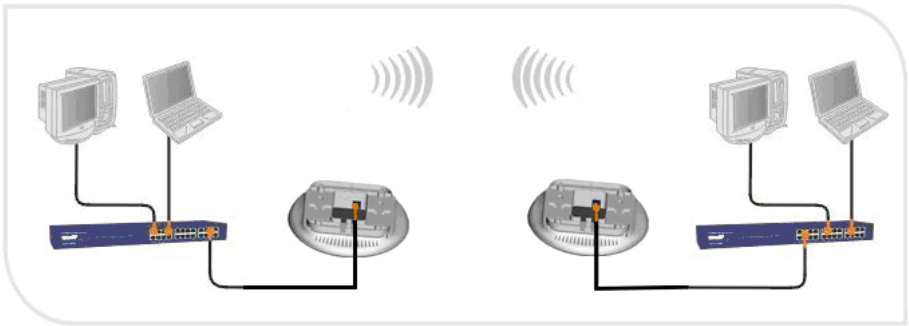
- ***BSSID:*** Basic Service Set Identifier of wireless network. In IEEE802.11, BSSID is the MAC address of wireless access point.
- ***WLAN Isolation:*** The access control feature based on wireless MAC address. When this feature is enabled, each of your wireless clients will be in its own virtual network and will not be able to communicate with each other. This feature is to isolate the communication of wireless clients connected with different ceiling AP.
- ***Channel:*** Specify the effective channel (from 1 to 13\Auto Select) of the wireless network.
- ***Extension Channel:*** To increase data throughput of wireless network, the extension channel range is used in 11n mode.
- ***Channel Bandwidth:*** Select the proper channel bandwidth to improve the wireless performance. 20M bandwidth can improve the anti-jamming ability of the wireless device. 40M bandwidth can improve the flux of 11N client.

4.1.2 Bridge (WDS) Mode

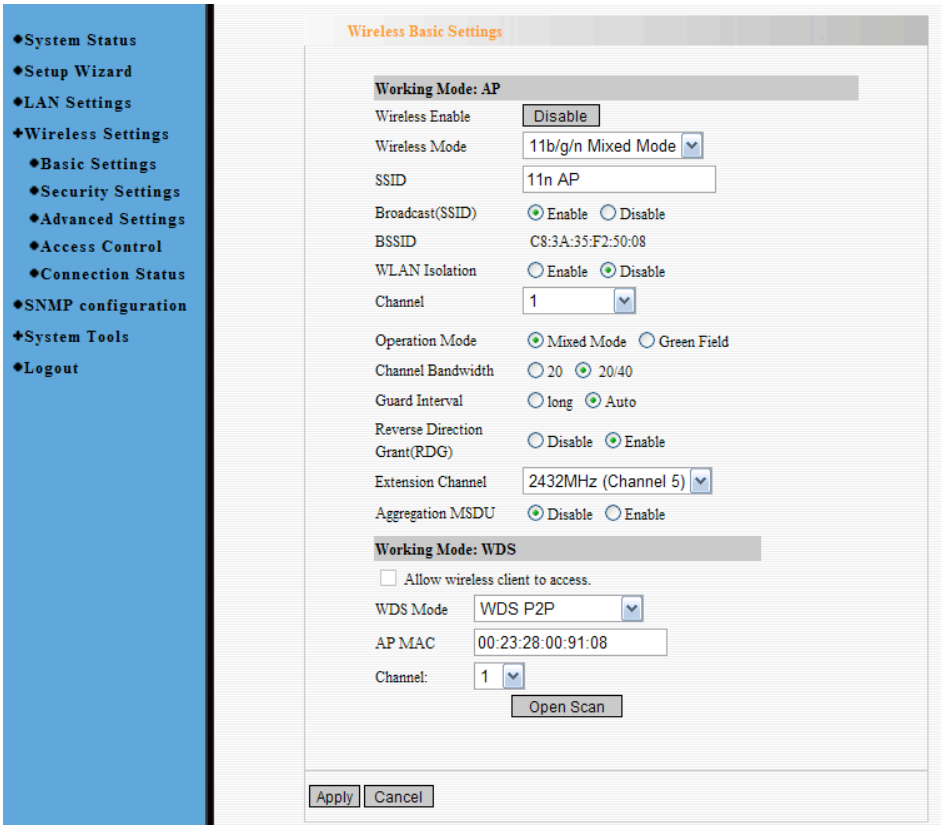
Bridge (WDS) mode includes **WDS P2P**, **WDS P2MP**, and **WDS AP Repeater**.

4.1.2.1 Point to Point Bridge

WDS P2P bridge mode can connect with two wired network via wireless access points, which communicate by wireless signals and not by cables. This mode can be free from the cable trouble. The P2P topology shows below:



Select **SSID broadcast** in drop-down list of WDS Mode as the picture below:



This page includes the AP and WDS parameter setting. AP parameter setting can change SSID and enable/ disable wireless feature.

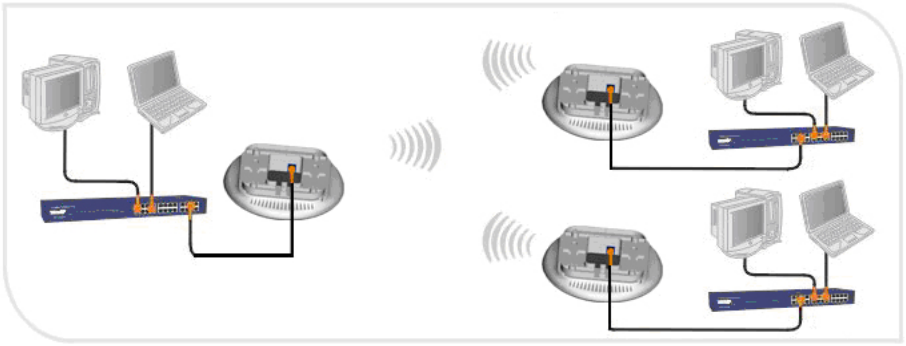
- ***AP MAC:*** Enter the interconnection equipment's MAC address.
- ***Channel:*** Select the channel according to interconnection equipment's; the ceiling AP on the two ends must be at the same channel.
- ***Open Scan:*** When you click this button, the ceiling AP will scan and list all the available wireless devices automatically. Select the device which need to bridge, it will add the device's MAC address automatically and select the corresponding channel.

4.1.2.2 P2MP Bridge Mode

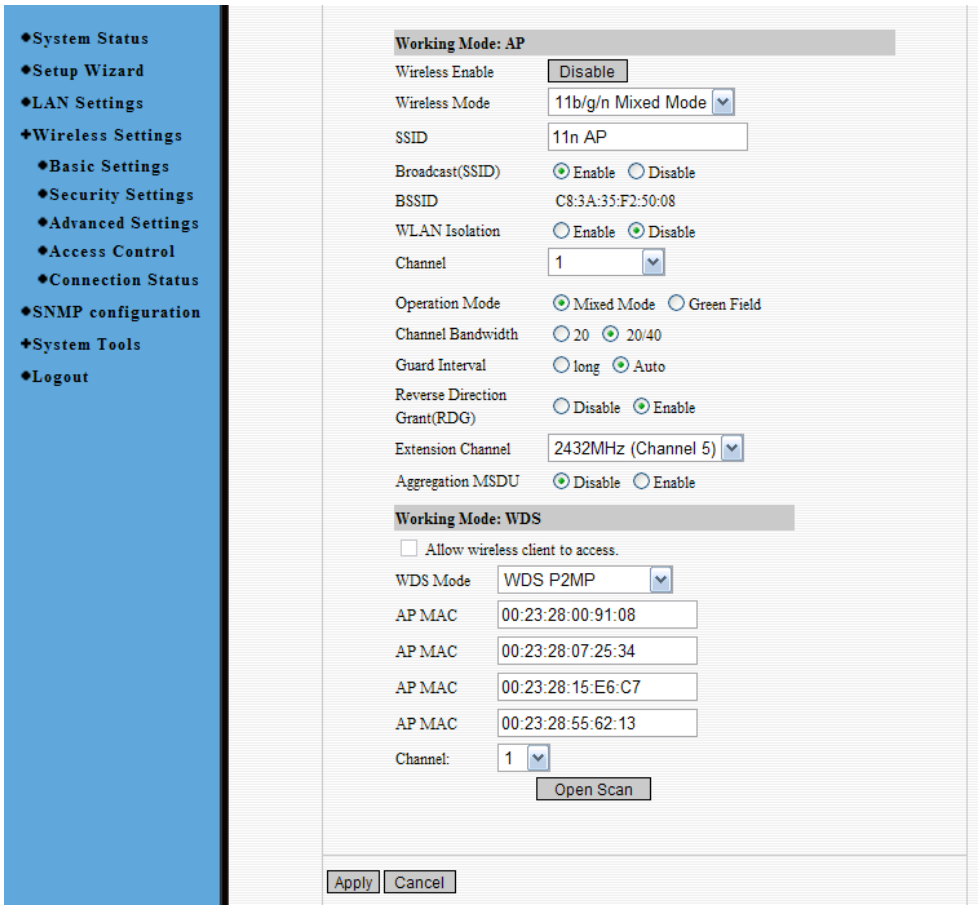
WDS P2MP bridge mode which connects scattered wired network together is more complicated than WDS P2P bridge mode. WDS P2MP usually transmits wireless signals from one access point, and other access points are in charge of receiving signals so as to share network resource. Support up to 4 remote ceiling AP connections. In this mode, wireless clients are not allowed to connect.

WDS P2MP bridge mode can connect multiple ceiling APs together without cabling. If the **Root AP** is configured as WDS P2MP bridge mode, other (less than 4) remote access points

should select **WDS P2P** bridge modes. The topology shows below:



Select **WDS P2MP** mode in the drop-down list of WDS Mode as the picture below.



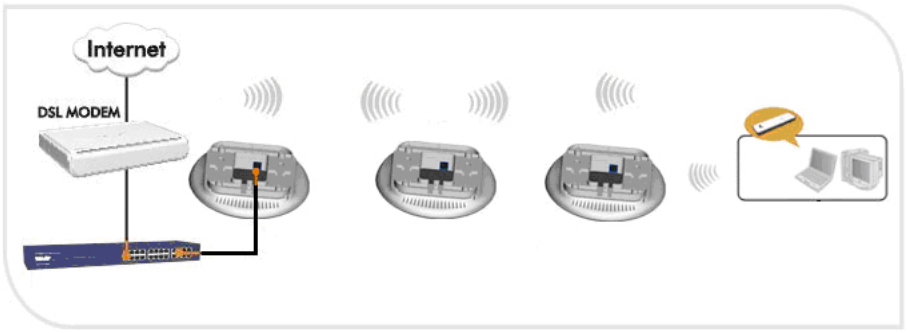
- ***AP MAC (Address):*** Input the remote AP's MAC address. (Maximum 4)
- ***Channel:*** Select the channel which bridge needs to use (all ceiling APs in the bridge must be at the same channel).
- ***Open Scan:*** When you lick this button, it will scan and list all the available wireless devices automatically. Select the device which need to bridge, it will add the device's MAC address automatically and select the corresponding channel. When multiple devices are added, it will select the channel of the last added ceiling AP as the bridge

used channel (you can also change the channel according to your need. All the ceiling APs must at the same channel in order to establish the connections).

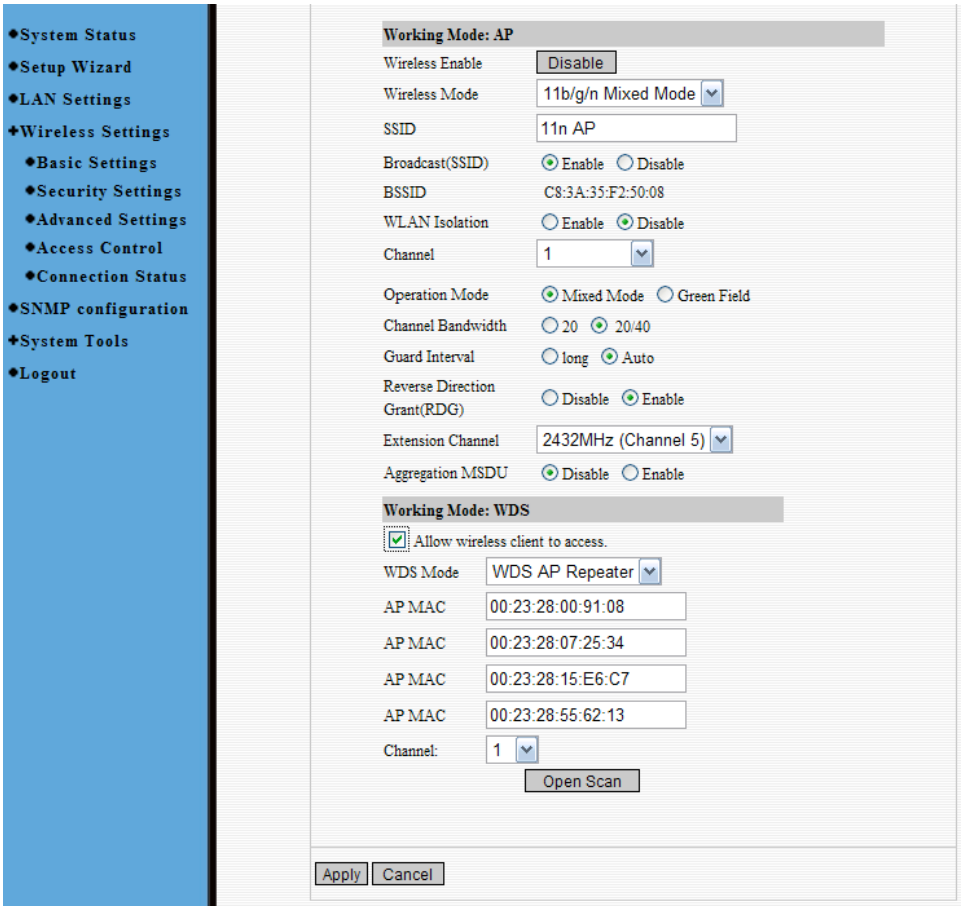
4.1.2.3 WDS AP Repeater Mode

WDS AP Repeater mode can repeat and amplify wireless signals to extend wireless network coverage. In this mode, wireless clients are allowed to connect.

When two LAN's transmission distance exceeds the wireless device's maximum transmission value, or there is much block among devices, you can use this mode to solve these problems by adding MAC addresses. The topology shows below:



Select **WDS AP Repeater** in the drop-down list of WDS Mode and the page will show as below.



When you select **Allow wireless client to access**, the ceiling AP can also be used as **Wireless Access Point** to allow the access of wireless client even when it works in bridge mode. There two parts of basic settings: one is the basic setting in AP mode (See 4.1.1.2); and another part is the basic setting in WDS mode (See 4.1.2.2).

4.2 Security Settings

It is used to configure the security settings, including AP security setting and WDS security setting.

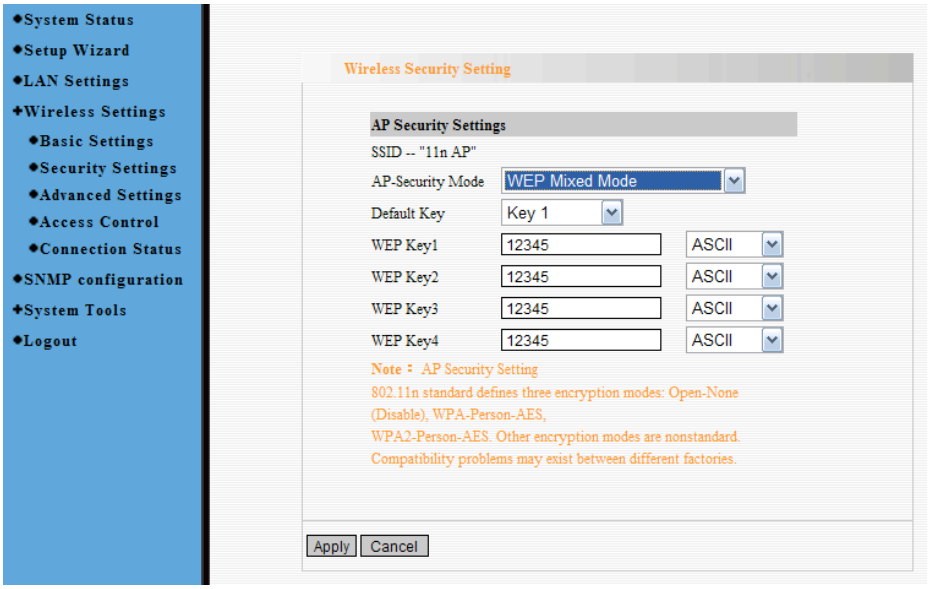
4.2.1 AP Security Setting

There are ten types of encryption modes; we introduce six of them which are the most common types, including **WEP Mixed Mode**, **WPA-Enterprise**, **WPA-PSK**, **WPA2-PSK**, **WPA2-Enterprise** etc.

WEP Mixed Mode

WEP (Wired Equivalent Privacy), a basic encryption method, usually encrypts wireless data using a series of digital keys (64 bits or 128 bits in length). By using the same keys on each of your wireless network devices, you can prevent unauthorized wireless devices from monitoring your transmissions or using your wireless resources. WEP is based on RSA

algorithm from RC4. It is the original and weak encryption method, so it is recommended not to use this method. Select **WEP Mixed mode** to enter the following page:

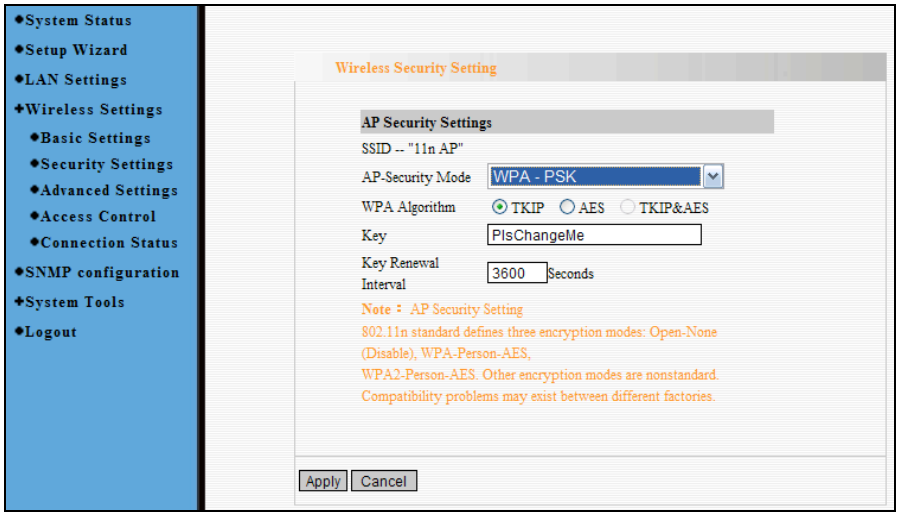


Setting Explanation

- ***AP Security Mode:*** Select the corresponding security encryption modes from the drop-down list.
- ***WEP Key1~4:*** Set the WEP key with the format of ASCII and Hex. You can enter ASCII code (5 or 13 ASCII characters. Illegal character as **"/"** is not allowed), or 10/26 hex characters.
- ***Default Key：*** Select one key out of four configured keys as the current available one.

WPA- PSK

WPA (Wi-Fi Protected Access), a Wi-Fi standard, is a more recent wireless encryption scheme, designed to improve the security features of WEP. Select **WPA-PSK** from the drop-down list to enter the following page:

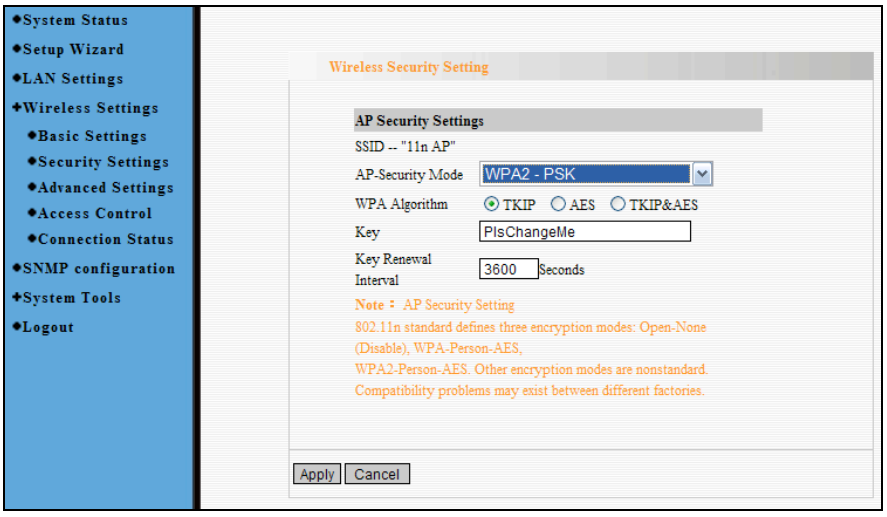


Setting Explanation

- ***WPA Algorithm:*** There are **TKIP** (Temporal Key Integrity Protocol), **AES** (Advanced Encryption Standard) and **TKIP&AES**. The default is TKIP mode.
- ***Key (Pass Phrase):*** Enter the encrypted characters with 8-63 ASCII characters.
- ***Key Renewal Interval:*** Set the key's renewal period.

WPA2-PSK

WPA2 provides more secured features than WEP and WPA. Select **WPA2-PSK** from the drop-down list to enter the following page:

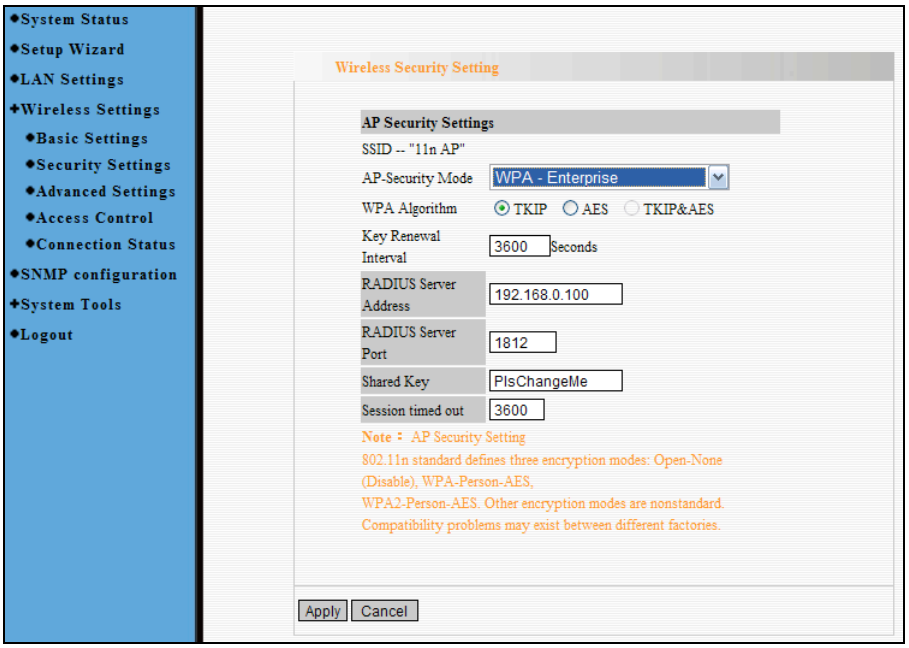


Setting Explanation

- ***WPA Algorithm:*** There are **TKIP** (Temporal Key Integrity Protocol), **AES** (Advanced Encryption Standard) and **TKIP&AES**. The default is TKIP mode.
- ***Key (Pass Phrase):*** Enter the encrypted characters with 8-63 ASCII characters.
- ***Key Renewal Interval:*** Set the key's renewal period.

WPA-Enterprise

This security mode is used when a RADIUS server is connected to the ceiling AP. Select **WPA-Enterprise** from the drop-down list to enter the following page:

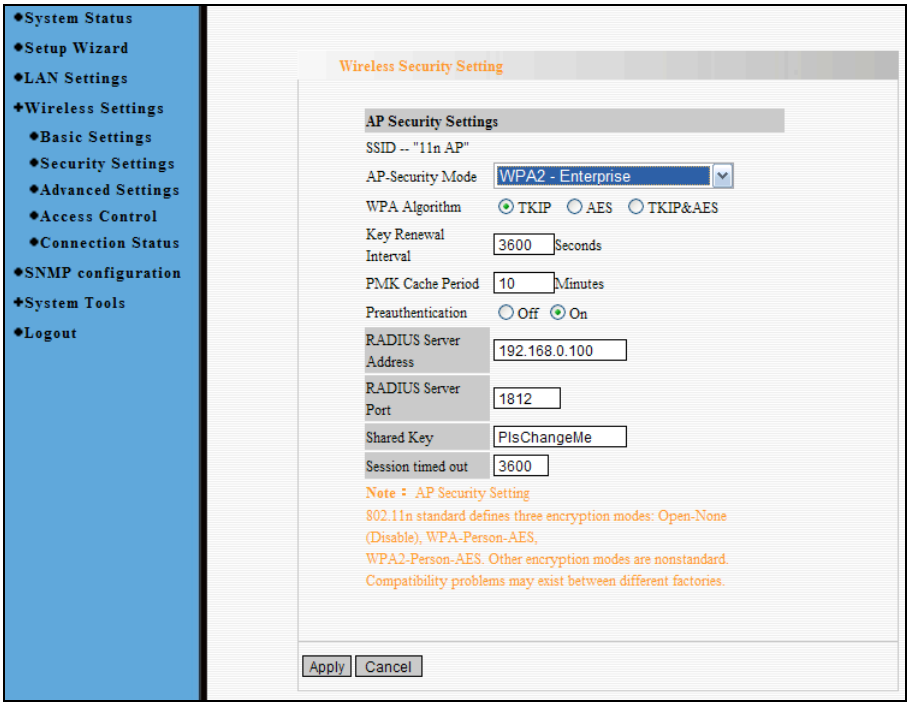


Setting Explanation

- ***WPA Algorithm:*** There are **TKIP** (Temporal Key Integrity Protocol), **AES** (Advanced Encryption Standard) and **TKIP&AES**. The default is TKIP mode.
- ***Key Renewal Interval:*** Set the key's renewal period.
- ***Radius Server Address:*** Enter the IP address of the Radius server.
- ***Radius Server Port:*** Enter the authentication port of the Radius server. The default is 1812.
- ***Shared Key:*** Enter the shared key for authentication server with 8~63 ASCII characters.
- ***Session timed out:*** The authentication interval period between ceiling AP and authentication server. The default is 3600s.

WPA2-Enterprise

This security mode is based on Radius authentication server and WPA2 encryption method, and when a RADIUS server is connected to the ceiling AP. Select **WPA2-Enterprise** from the drop-down list to enter the following page:

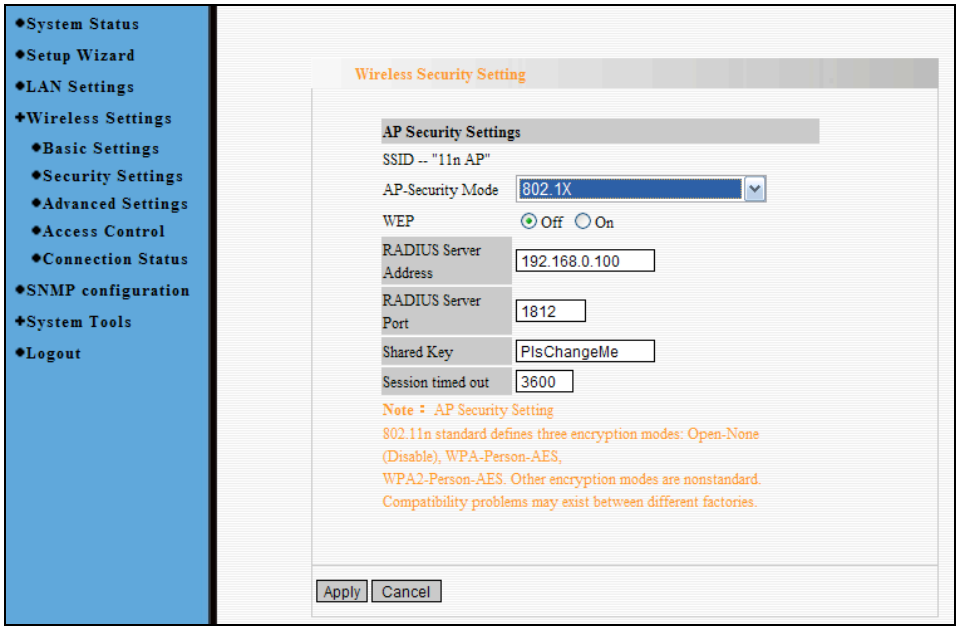


Setting Explanation

- ***WPA Algorithm:*** There are **TKIP** (Temporal Key Integrity Protocol), **AES** (Advanced Encryption Standard) and **TKIP&AES**. The default is TKIP mode.
- ***Key Renewal Interval:*** Set the key's renewal period.
- ***Radius Server Address:*** Enter the IP address of the Radius server.
- ***Radius Server Port:*** Enter the authentication port of the Radius server. The default is 1812.
- ***Shared Key:*** Enter the shared key for authentication server with 8~63 ASCII characters.
- ***Session timed out:*** The authentication interval period between ceiling AP and authentication server. The default is 3600s.

802.1X Authentication

This security mode is used when a RADIUS server is connected to the ceiling AP. 802.1x, a kind of Port-based authentication protocol, is an authentication type and strategy for users. The port can be either a physic port or logic port (such as VLAN). For wireless LAN users, a port is just a channel. The final purpose of 802.11x authentication is to check if the port can be used. If the port is authenticated successfully, you can open this port which allows all the messages to pass. If the port isn't authenticated successfully, you can keep this port **disable** which just allows 802.1x authentication protocol message to pass. Select **802.1X** from the drop-down list to enter the following page:



Setting Explanation

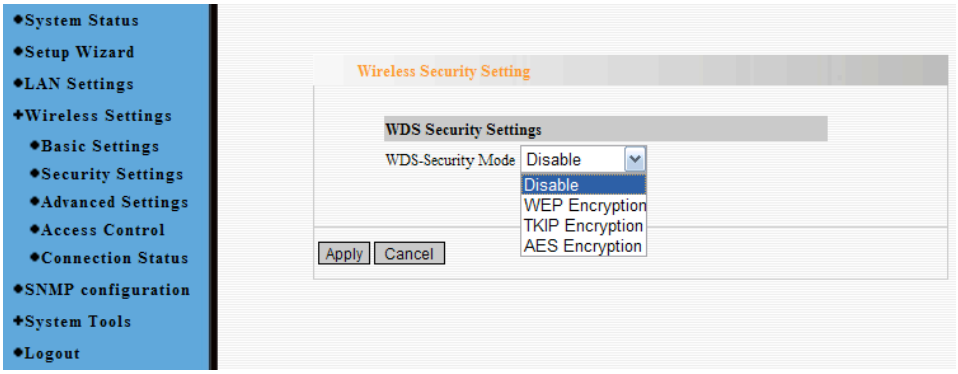
- ***WEP:*** Click **On/Off** to enable or disable the WEP algorithm.
- ***Radius Server Address:*** Enter the IP address of the Radius server.
- ***Radius Server Port:*** Enter the authentication port of the Radius server. The default is 1812.
- ***Shared Key:*** Enter the shared key for authentication server with 8~63 ASCII characters.
- ***Session timed out:*** The authentication interval period between ceiling AP and authentication server. The default is 3600s.

Note: To improve security level, do not use too easy characters.

4.2.2 WDS Security Setting

WDS Security Setting is to protect the data safety of wireless bridge.

The security setup page of Point to Point Bridge and Point to Multipoint Bridge is as the picture below:

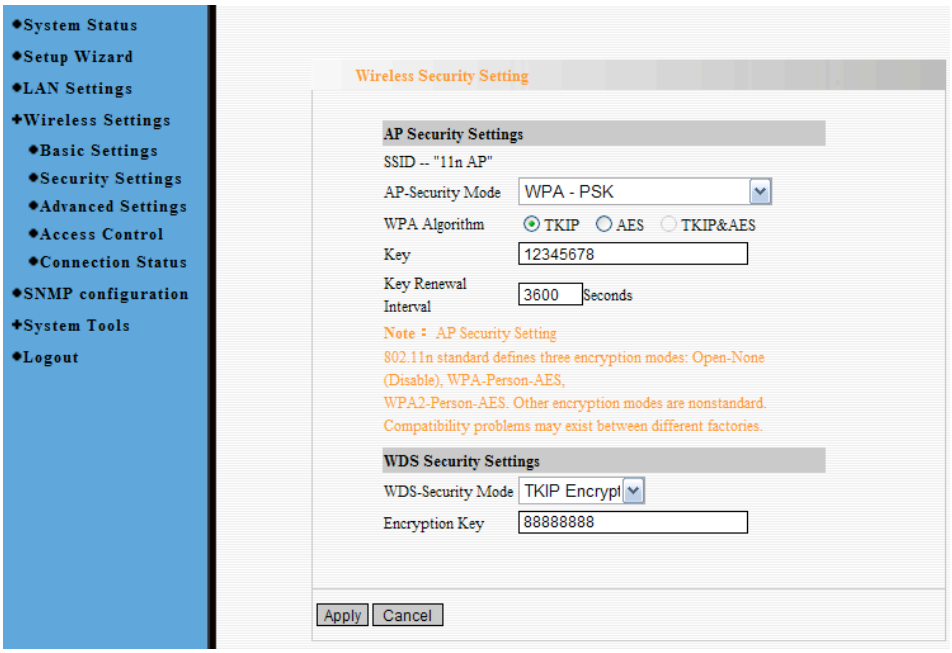


WDS security setting provides three encryption modes: **WEP**, **TKIP**, and **AES** encryption.

- ***WEP Key:*** You can set the WEP key in ASCII code or Hexadecimal code.
- ***Key:*** You can choose ASCII code (5 or 13 ASCII codes, illegal characters like **"/"** are forbidden) or Hexadecimal characters (10 or 26 Hexadecimal characters).
- ***TKIP/ AES Encryption Key:*** TKIP/AES is an encryption mode based on WPA and WPA2.
- ***Key:*** Key characters are ASCII codes from 8 to 63.

Note: **The encryption mode and password of each ceiling AP in the bridge must be consistent in order to establish the connections. You are recommended to encrypt the bridge to protect the wireless bridge.**

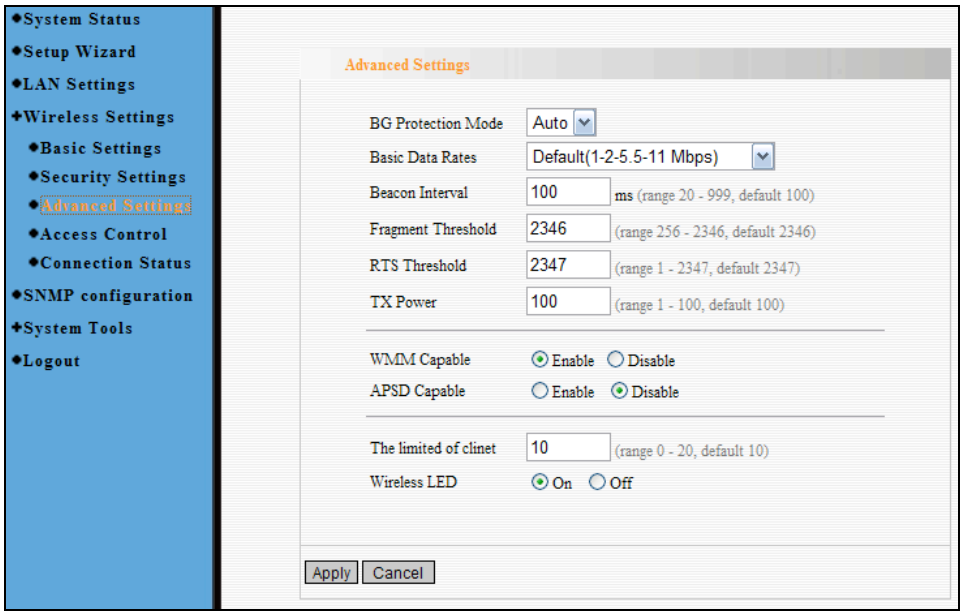
The security setup page of wireless repeater is as follow:



There are two parts of security setting in **WDS AP Repeater** mode: **AP Security Settings** and **WDS Security**. AP security setting focuses on wireless client access, while WDS security setting focuses on wireless bridge connection. AP security setting appears only when wireless client accesses are permitted in wireless repeater mode. Please refer to Chapter 4.2.1 for AP Security Setting.

4.3 Advanced Settings

This section mainly deals with wireless advanced settings, including Basic Data Rate, Beacon Interval, and Fragment Threshold etc. Select **Wireless Settings** -> **Advanced Settings** to enter the following page:

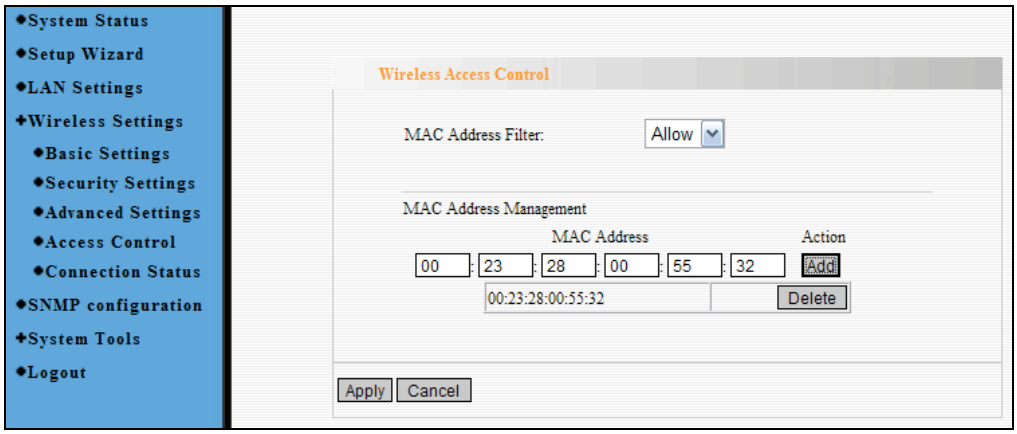


Setting Explanation

- ***BG Protection Mode:*** For 11b/g wireless client, it is easier to connect with 11n wireless device. The default is **Auto**.
- ***Basic Data Rates:*** In term of different requirements, you can select one of the suitable Basic Data Rates from the drop-down list. **Default (1-2-5.5-11Mbps)** is the default setting. It is recommended not to change the default value.
- ***Beacon Interval:*** The frequency interval of the beacon, which is a packet broadcast by an AP to synchronize a wireless network. The default value is 100ms.
- ***Fragment Threshold:*** The fragmentation threshold defines the maximum transmission packet size in bytes. The packet will be fragmented if the arrival is bigger than the threshold setting. The default size is 2346 bytes.
- ***RTS Threshold:*** RTS stands for **Request to send**. This parameter controls what size data packet the frequency protocol issues to RTS packet. If the device works in SOHO, do not change the default value.
- ***TX Power:*** Set the wireless output power level. The default value is 100.
- ***WMM Capable:*** To enhance wireless multimedia transfer performance (0n-line video and voice). If you are not clear about this, enable it.
- ***APSD Capable:*** It is used for auto power-saved service. The default is **Disable**.

4.4 Access Control

To secure your wireless LAN, the wireless access control is actually based on the MAC address management. Select **Wireless Settings** -> **Access Control** to display the following page:



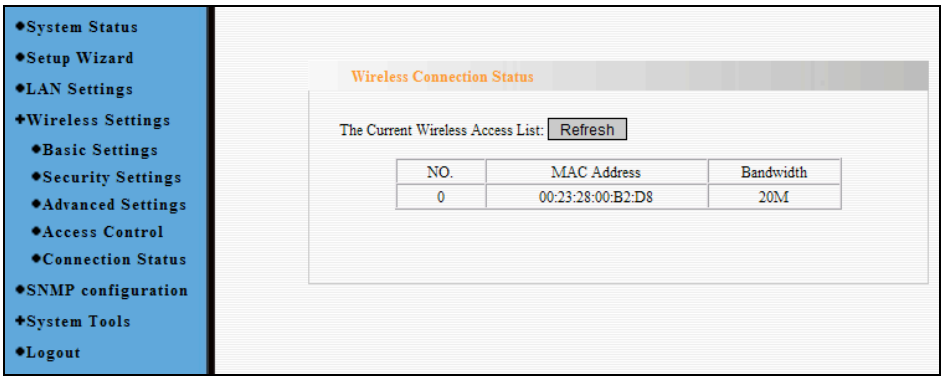
Setting Explanation

- ***MAC Address Filter:*** Enable or disable MAC address filter by selecting **Close**, **Allow**, or **Block**. Select **Close** to malfunction MAC address; **Block** to prevent the MAC addresses in the list from accessing the wireless network; **Allow** to allow the MAC address in the list to access the wireless network.
- ***MAC Address Management:*** Input the MAC address to implement the filter policy. Click **Add** to finish this setting.
- ***MAC List:*** Shows the MAC addresses added. You can add or delete them.

Note: Ceiling AP supports no more than 32 MAC addresses.

4.5 Connection Status

This page shows wireless client's connection status, including MAC address, Channel bandwidth etc. Select **Wireless Settings** -> **Connection Status** to the following page:



Setting Explanation

- ***MAC Address:*** Shows current connecting host's MAC address.
- ***Bandwidth:*** Shows current connecting host's (wireless client) bandwidth (20MHz or 40MHz).

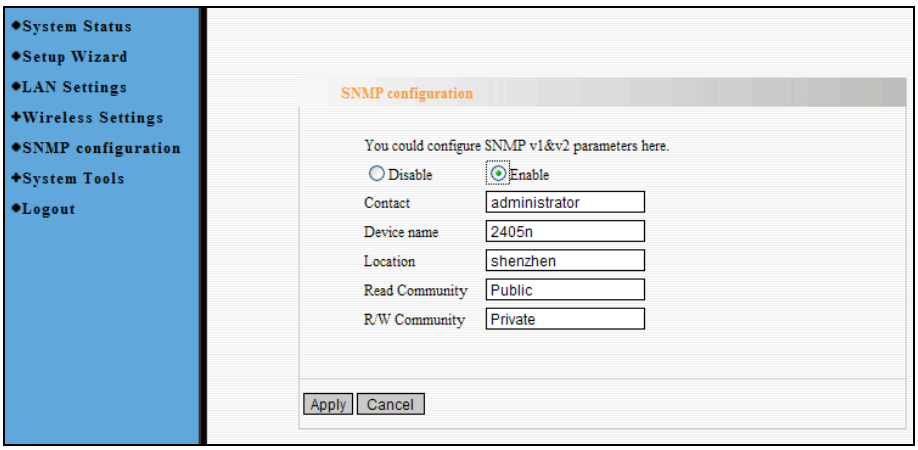
Chapter 5 SNMP Configuration

5.1 SNMP Introduction

Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is widely used in local area networks (LAN) for collecting information, and managing and monitoring, network devices, such as servers, printers, hubs, switches, and routers from a management host. Managed devices that support SNMP including software are referred to as an SNMP agent, which usually interacts with third-party SNMP management software to enable the sharing of network status information between monitored devices and applications and the SNMP management system. A defined collection of variables (managed objects) are maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

5.2 SNMP Setting

This device supports SNMP v1 and SNMP v2c. Please click **SNMP Configuration** to enter the following page:



Click **Enable** or **Disable** to turn on or turn off SNMP management.

Setting Explanation

- ***Contact:*** Set the name to access the ceiling AP. Usually set the administrator's name.
- ***Device Name:*** Set a name for this ceiling AP, for example, 2405n.
- ***Location:*** Set the network location for this ceiling AP.

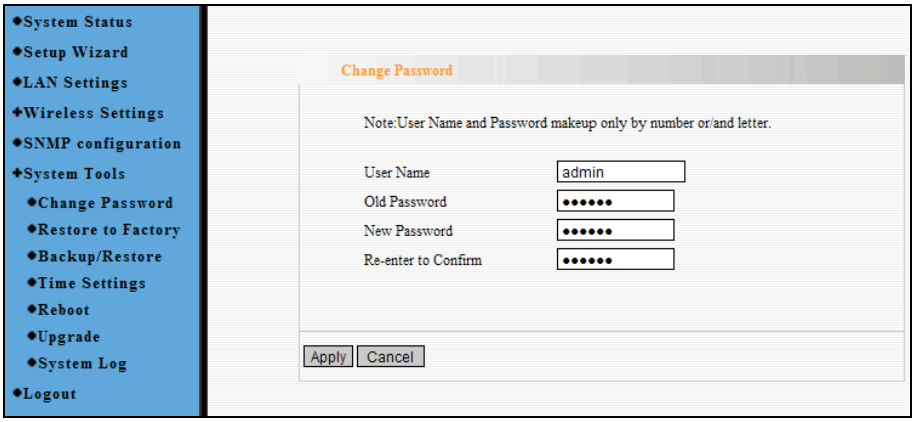
- ***Read Community:*** Indicates the community read access string to permit reading this ceiling AP's SNMP information. The default is **Public**.
- ***R/W (Read/Write) Community:*** Indicates the community read/write access string to permit reading and re-writing this ceiling AP's SNMP information. The default is **Private**.

Chapter 6 System Tools

This section focuses on how to maintain ceiling AP. Including Change Password, Restore to Factory, Backup/Restore, Upgrade (firmware), Reboot, and System Log.

6.1 Change Password

This section is to set a new user name and password to better secure your ceiling AP and network. Click **Apply** after you complete.



- ***User Name:*** Enter a new user name for the device.
- ***Old Password:*** Enter the old password.
- ***New Password:*** Enter a new password.
- ***Re-enter to Confirm:*** Re-enter to confirm the new password.

NOTE*:* It is highly recommended to change the password to secure your network and the ceiling AP.

6.2 Restore to Factory

This is to reset all configurations to the default values. It means the ceiling AP will lose all the settings you have set.

Restore: Click this button to restore to default settings.

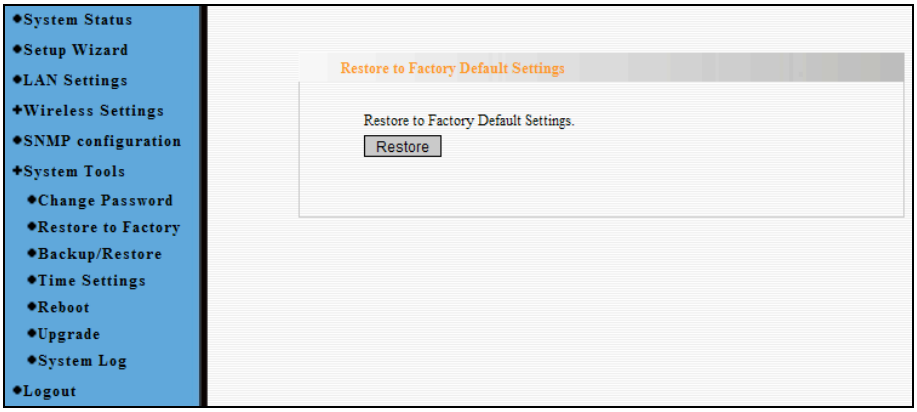
Factory Default Settings:

User Name: admin

Password: admin

IP Address: 192.168.0.254

Subnet Mask: 255.255.255.0



6.3 Backup/Restore

The ceiling AP provides backup/restore settings; please specify a location to keep these settings.

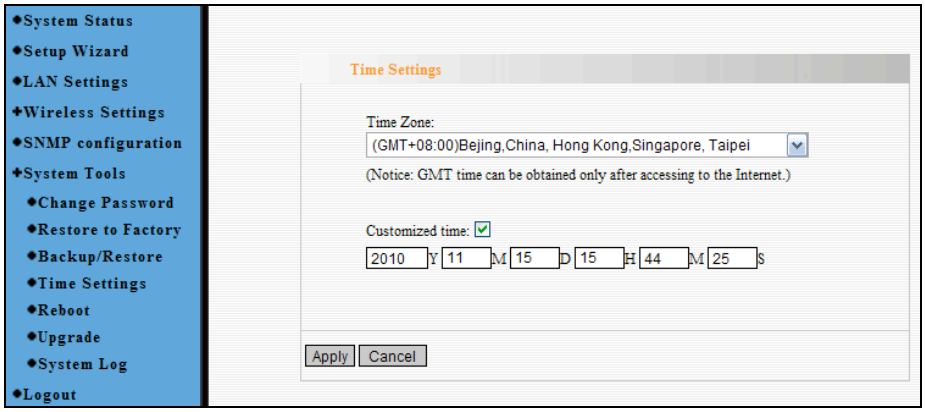
Backup: Click this button to back up all the configurations.

Browse: Click this button to browse the directory where you want to save the configurations.

Restore: Click this button to restore the ceiling AP's configurations.

6.4 Time Settings

This section is to select the time zone for your location. You can select your own time or obtain the standard GMT time from Internet.



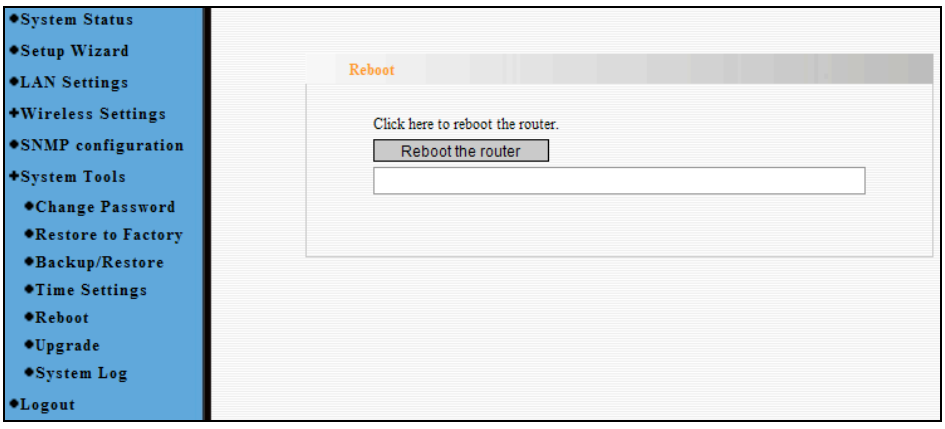
Setting Explanation

- ***Time Zone:*** Select your time zone from the drop-down list.
- ***Customized time:*** Enter the time you customize.

6.5 Reboot

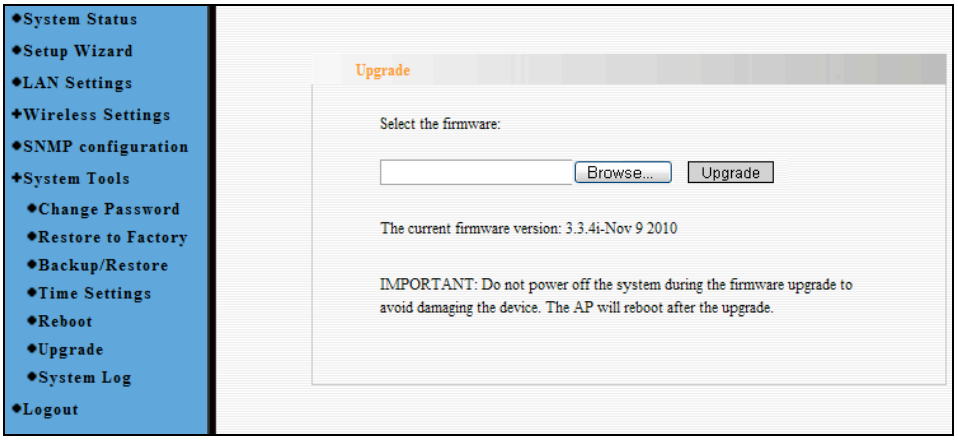
This page is used to reboot ceiling AP. Rebooting the ceiling AP makes the settings configured go into effect.

Reboot: Click this button to reboot the ceiling AP.



6.6 Firmware Upgrade

Firmware will be available by e-mail request. Please contact your local agent on this matter. After the upgrade is completed, the ceiling AP will reboot automatically.



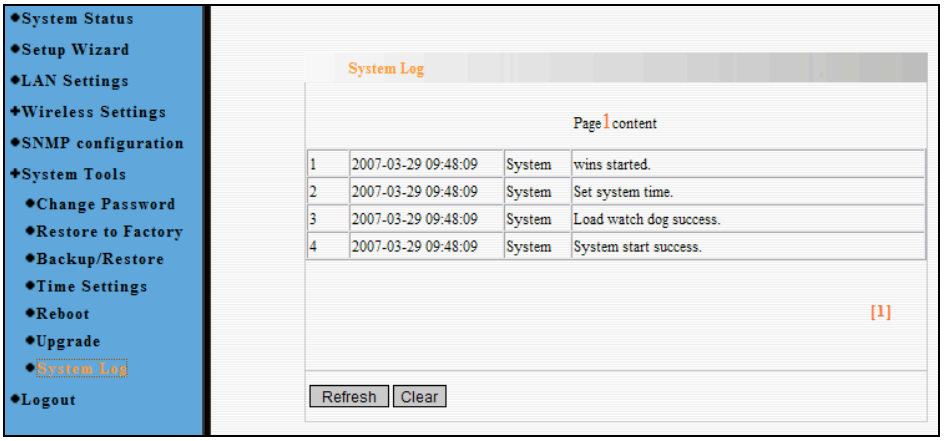
Upgrade Steps：

1. Select **Upgrade**, enter the complete path of the firmware location, or click the **Browse** to find the file.
2. Click **Upgrade** and follow the instructions.
3. After the upgrade is completed, the ceiling AP will reboot automatically.

IMPORTANT: Do not power off the system during the firmware upgrade to avoid damaging the ceiling AP.

6.7 System log

The section is to view the system log. Click **Refresh** to update the log. Click **Clear** to clear all shown information. If there are more than 150 records, it will clear them automatically.



Refresh: Click this button to update the log.

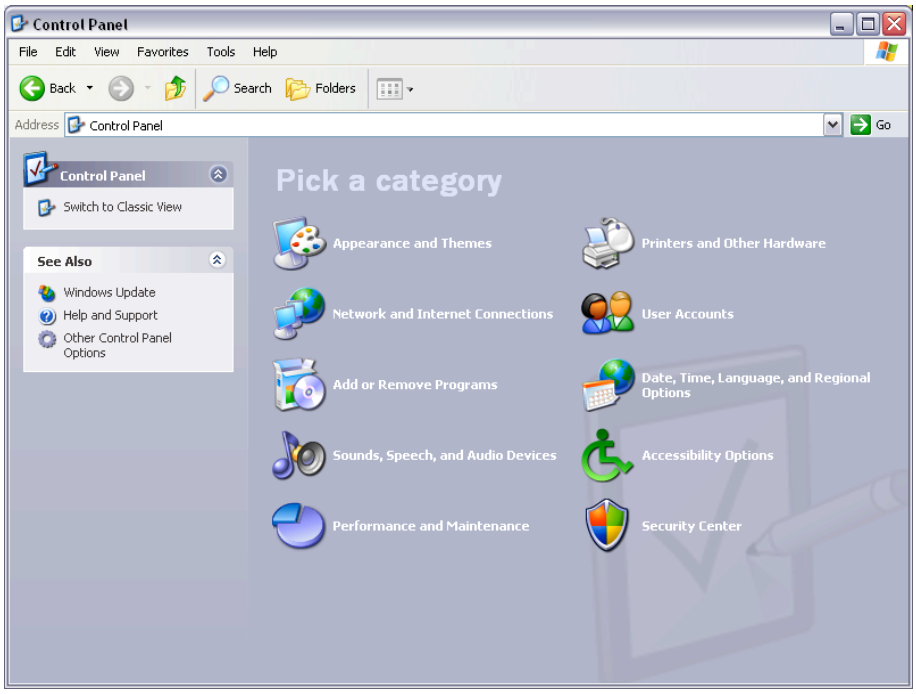
Clear: Click this button to clear the current log.

Appendix I: Glossary

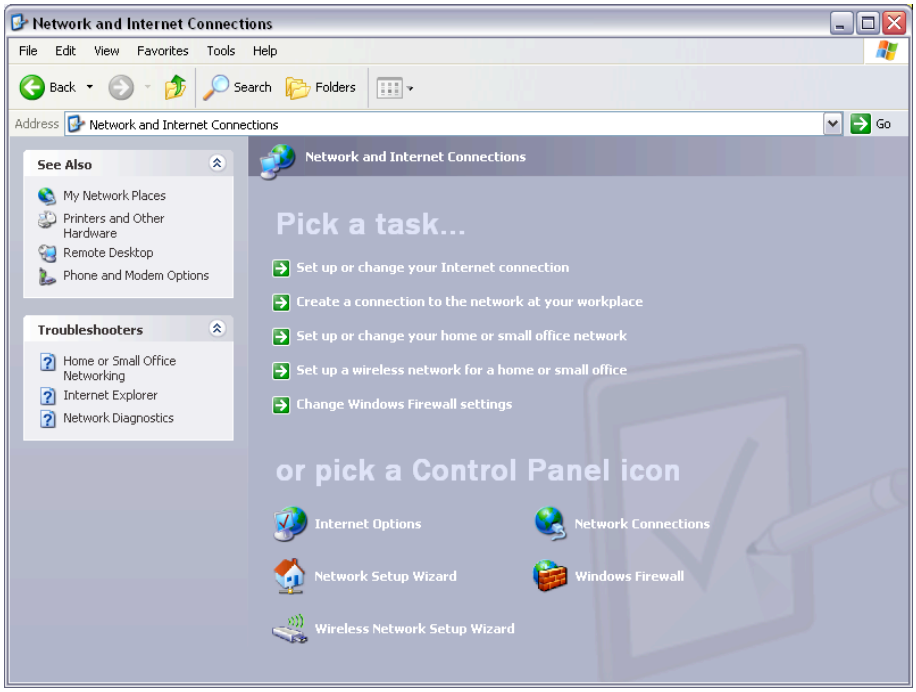
Access Point (AP): Any entity that has station functionality and provides access to the distribution services, via the wireless medium (WM) for associated stations.
Channel: An instance of medium use for the purpose of passing protocol data units (PDUs) that may be used simultaneously, in the same volume of space, with other instances of medium use(on other channels) by other instances of the same physical layer (PHY),with an acceptably low frame error ratio(FER) due to mutual interference.
SSID: Service Set identifier. An SSID is the network name shared by all devices in a wireless network. Your network's SSID should be unique to your network and identical for all devices within the network. It is case-sensitive and must not exceed 20 characters (use any of the characters on the keyboard).Make sure this setting is the same for all devices in your wireless network.
WEP: Wired Equivalent Privacy (WEP) is the method for secure wireless data transmission. WEP adds data encryption to every single packet transmitted in the wireless network. The 40bit and 64bit encryption are the same because of out 64 bits, 40 bits are private. Conversely, 104 and 128 bit are the same. WEP uses a common KEY to encode the data. Therefore, all devices on a wireless network must use the same key and same type of encryption. There are 2 methods for entering the KEY; one is to enter a 16-bit HEX digit. Using this method, users must enter a 10-digit number (for 64-bit) or 26-digit number (for 128-bit) in the KEY field. Users must select the same key number for all devices. The other method is to enter a text and let the computer generate the WEP key for you. However, since each product use different method for key generation, it might not work for different products. Therefore, it is NOT recommend using.
WPA/WPA2: A security protocol for wireless networks that builds on the basic foundations of WEP. It secures wireless data transmission by using a key similar to WEP, but the added strength of WPA is that the key changes dynamically. The changing key makes it much more difficult for a hacker to learn the key and gain access to the network.WPA2 is the second generation of WPA security and provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some government users.

Appendix II: TCP/IP Address Setting (Take Windows XP for example)

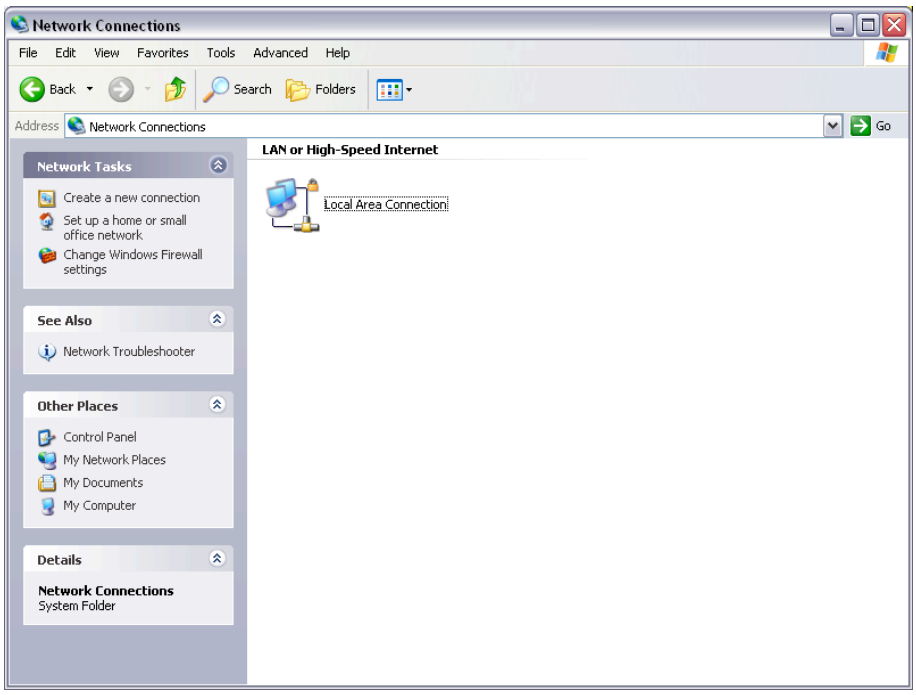
Click **Start** > **Settings** > **Control Panel** > **Network and Internet Connections**.



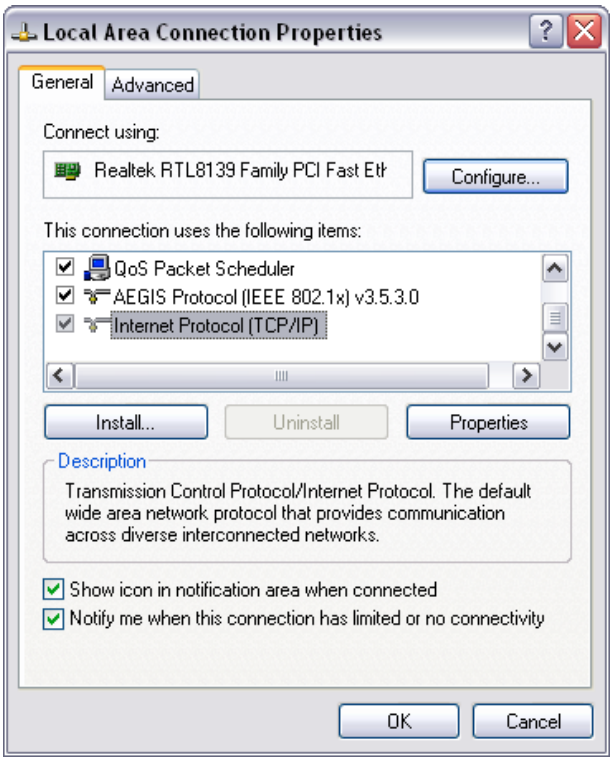
Click **Network Connections**.


Network and Internet Connections
File Edit View Favorites Tools Help
Back Search Folders
Address Network and Internet Connections
Go
See Also
My Network Places
Printers and Other Hardware
Remote Desktop
Phone and Modem Options
Troubleshooters
Home or Small Office Networking
Internet Explorer
Network Diagnostics
Network and Internet Connections
Pick a task...
Set up or change your Internet connection
Create a connection to the network at your workplace
Set up or change your home or small office network
Set up a wireless network for a home or small office
Change Windows Firewall settings
or pick a Control Panel icon
Internet Options
Network Connections
Network Setup Wizard
Windows Firewall
Wireless Network Setup Wizard

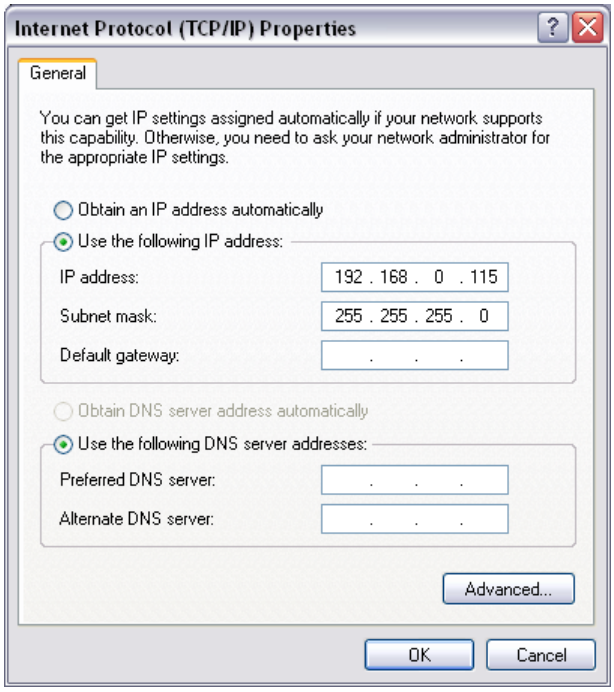
Right click on **Local Area Connection**, and clink **Properties**.



Click **Internet Protocol (TCP/IP)** > **Properties**.



Choose the **Use the following IP address** and enter the IP address as: 192.168.0.xxx (xxx ranges 1~253), Subnet mask: 255.255.255.0.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 0 . 115
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Click **OK** to apply and return to **Local Area Connection Properties**.

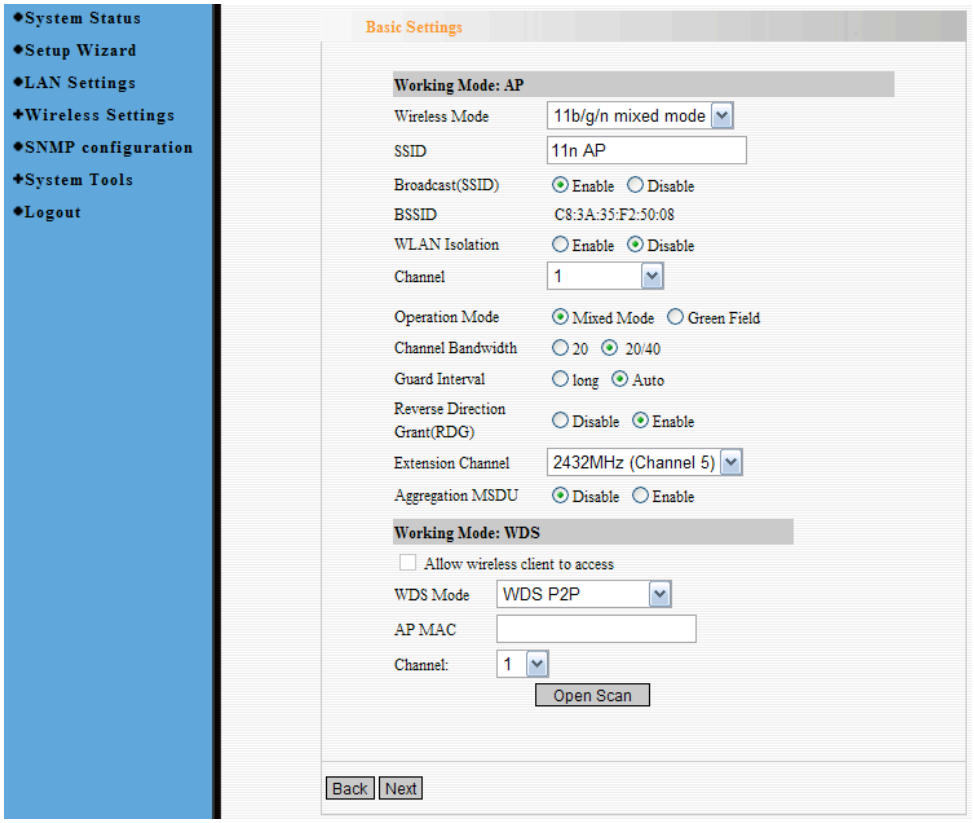
Continue click **OK** to exit the setting windows.

Appendix III: WDS Application Instances

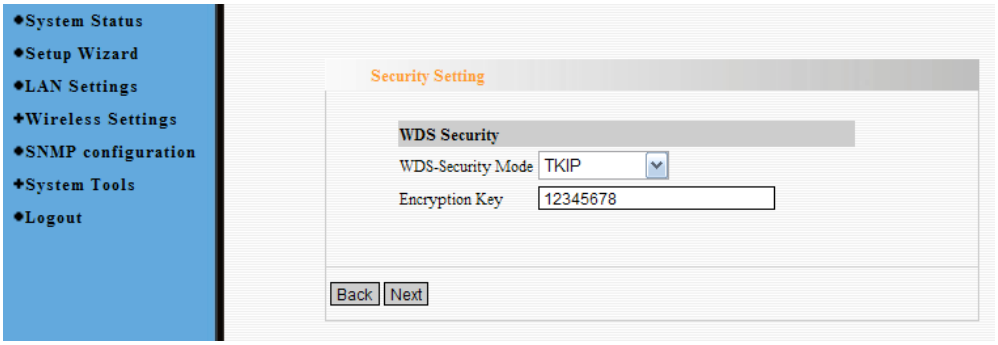
The configurations of P2P, P2MP and Wireless Repeater in WDS mode are mostly the same. The number of devices which need to be configured is different according to different mode. The following steps take **P2P** for example.

If you want to establish P2P transmission between AP1 and AP2, you need to set the parameters as follows:

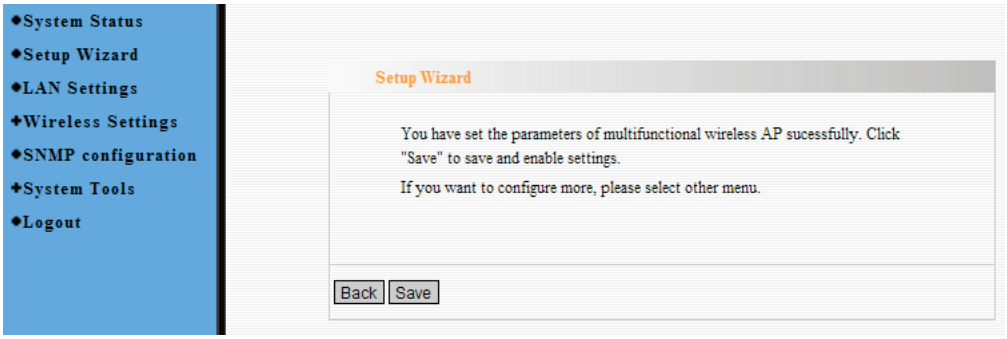
Select **WDS** mode in **Setup Wizard** for AP1 and set the SSID as **AP1** and select channel **1**. The BSSID is 00:23:28:05:4E:D0.



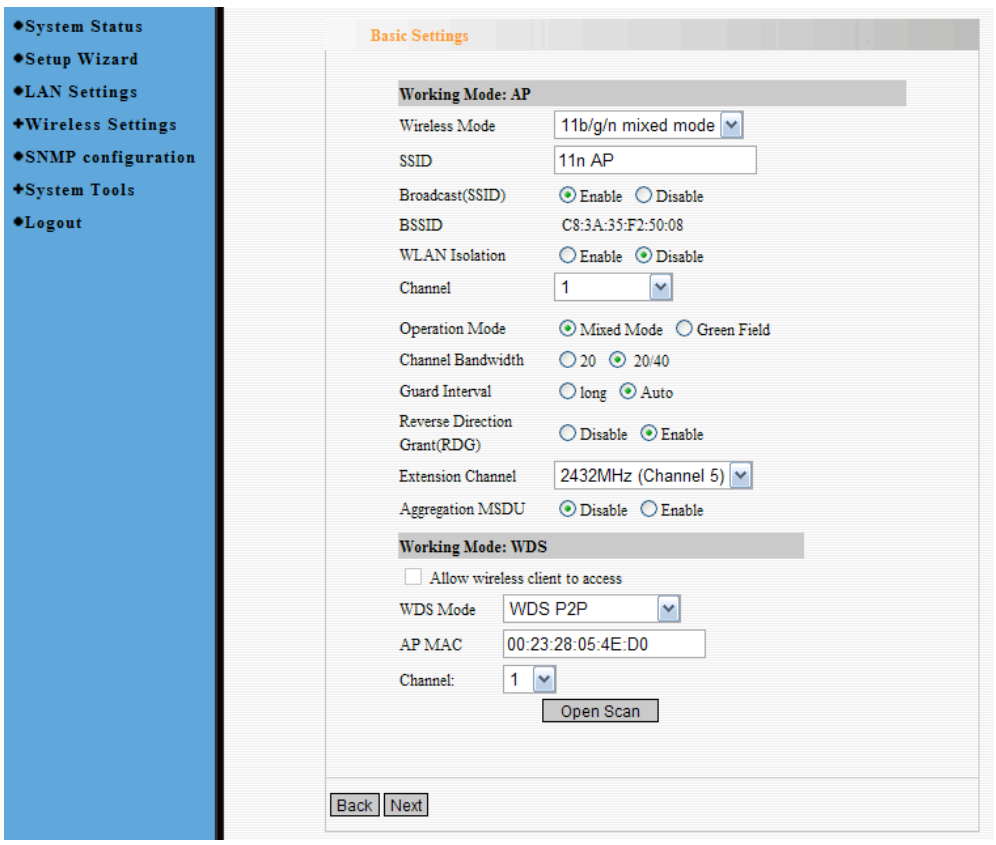
Click **Next** to enter the **WDS Security** setting.



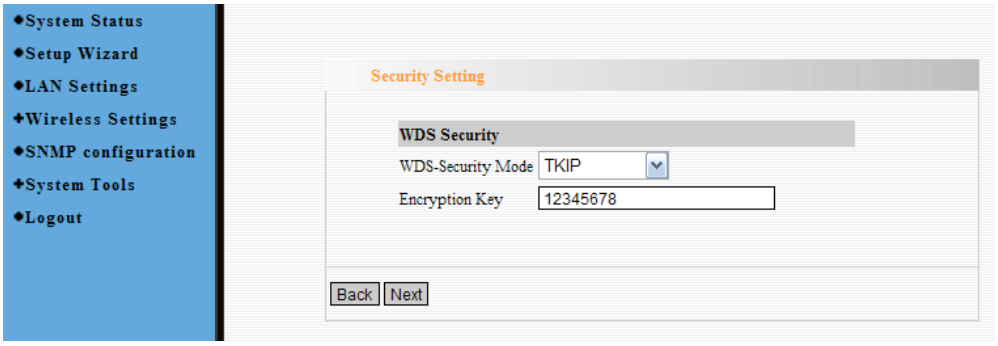
Select the encryption mode you want to use (For example: set the encryption mode as **TKIP** and enter the encryption key as 12345678).



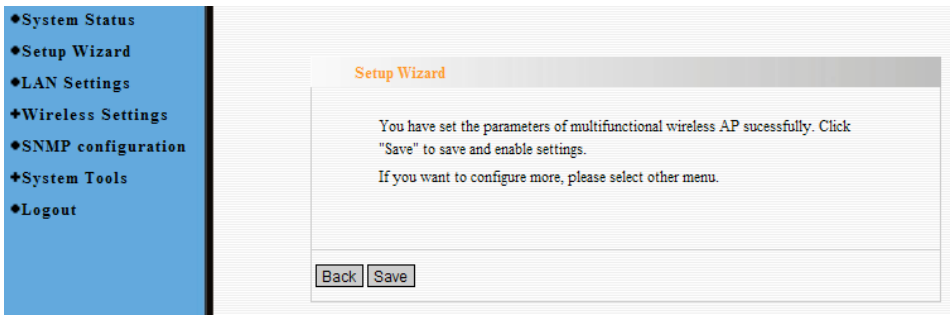
Click **Next** and **Save** to complete the settings. Then login AP2 for settings:
Select **WDS** mode for AP2 and set SSID as **AP2**. Select channel **1** as the same as AP1. Enter BSSID: 00:23:28:05:4E:D0 of AP1 into the AP MAC blank and record the BSSID 00:23:28:F2:50:08 of AP2. (You can also use **Open Scan** to find AP1).



Click **Next** to enter the **WDS Security** setting and select AP1 corresponding encryption mode. Then enter the encryption key (we select TKIP and encryption key 12345678).



Click **Next** and **Save** to complete the settings.



After you finished AP2 settings, return to AP1 setting:

Select **Wireless Settings** > **Basic Settings**, do not change SSID, channel and extension channel. You only need to enter BSSID：00:b0:c6:05:4e:dd of AP2 in AP MAC address blank an then save it (you can also use **Open Scan** to find AP2). Now you have completed all the settings of P2P.